The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/11/2016

SUBJECT:
A Vulnerability in vBulletin Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in vBulletin that could allow for remote code execution. vBulletin is a commercial forum and blog platform. Successful exploitation could result in sensitive information disclosure, sending spam, denial of service, data loss and remote code execution.

THREAT INTELLIGENCE:
There are unconfirmed reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:
- Versions prior to 3.8.9, 4.2.3, and 5.2.3 are vulnerable.

RISK:
Government:
- Large and medium government entities: **High**
- Small government: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: N/A

TECHNICAL SUMMARY:
A vulnerability has been discovered in vBulletin that could allow for remote code execution. If successful, the exploit can expose internal services on the network, and unauthenticated users or automated scanners would be able to send malicious data. This is the result of an issue in the vBulletin codebase that allows for HTTP redirects. As a result, vBulletin is susceptible to a server side request forgery attack. Successful exploitation could result in sensitive information disclosure, sending spam, denial of service, data loss and remote code execution.

Due to the imminent release of PHP 7.1, vBulletin 5.2.3 will be the last version of vBulletin to support PHP 5.4.X.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by vBulletin to vulnerable systems immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.

REFERENCES:

vBulletin:

http://www.vbulletin.com/forum/forum/vbulletin-announcements/vbulletin-announcements_aa/4349606-vbulletin-5-2-3-connect-is-now-available

Security Affairs:

http://securityaffairs.co/wordpress/50206/hacking/vbulletin-patches.html